CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 3, No. 1
April 2024
ISSN: 2832-1006

In this issue:

4. **A Mixed-Method Study Exploring Student Motivation for Participating in Cybersecurity CTF Competitions**
Cheryl Beauchamp, Regent University
Holly Matusovich, Virginia Tech

27. **Higher Education Model for Security Literacy using Bloom's Revised Taxonomy**
Gary White, Texas State University

37. **Comprehensive Cybersecurity Programs: Case-Study Analysis of a Four-Year Cybersecurity Program at a Secondary Education Institution in Arizona**
Paul Wagner, University of Arizona
Dalal Alharthi, University of Arizona

64. **Doing Postphenomenology in Cybersecurity Education: A Methodological Invitation**
Ryan Straight, University of Arizona

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

2024 Review Board

Doing Postphenomenology in Cybersecurity Education: A Methodological Invitation

Ryan Straight
ryanstraight@arizona.edu
Department of Cyber, Intel, & Information Operations
University of Arizona
Tucson, AZ 85721

Abstract

As the cyber domain grows into each aspect of our lives, so does the need to expand approaches in understanding and researching cybersecurity and cybersecurity education. By focusing on a novel methodology within these fields—postphenomenology—this paper seeks to demonstrate its cyber-related usefulness and application. At its core, postphenomenology is the study of technological mediation and the myriad ways of uncovering and understanding it and its consequences. In tracing a line from classic phenomenology to the exploration of cyborg technological intentionality, I suggest an applied postphenomenology that addresses calls for holistic and multidisciplinary cybersecurity education. By incorporating postphenomenological methods into cybersecurity pedagogical research and practice, educators and students alike can come to deeper and more meaningful realizations and applications stemming from human-technology-world relations.

Keywords: postphenomenology, methodology, mediation theory, intentionality, phenomenology, multidisciplinarity

Recommended Citation: Straight, R., (2024**).** Doing Postphenomenology in Cybersecurity Education: A Methodological Invitation. *Cybersecurity Pedagogy and Practice Journal*, 3(1), pp.64. https://doi.org/10.62273/TWSH7587

1. INTRODUCTION

As cybersecurity and cybersecurity education are still relatively nascent fields, a multidisciplinary and varied approach is appropriate to understanding and identifying opportunities to fill gaps and respond to needs unknown. This paper seeks to provide one such approach, bringing the lens of postphenomenology to bear on the process. Through "classical" phenomenology, Ihde's postphenomenology, and Rosenberger's and Verbeek's expansions thereof, and the work of others, I argue for the application of Adams and Turville's "postphenomenology of practice" to cybersecurity education. To achieve this, I provide a brief introduction to phenomenology and its connection to technology before delving into postphenomenology, an empirical philosophy of technology that explores the relation between humans, technology, and the world. I will then present postphenomenology's potential impact on the cybersecurity domain and apply postphenomenology to cybersecurity education, specifically. Suggestions for postphenomenological approaches to cybersecurity pedagogy and potential topics for analysis follow. First, however, I will explore the foundational cybersecurity education landscape.

2. NEEDS IN CYBERSECURITY AND CYBERSECURITY EDUCATION

Cybersecurity is, unsurprisingly, entirely reliant on *people* and *technology*. Without either, there is no cyber domain. However ubiquitous technology may be within the field, access to education is often strikingly lacking in breadth and depth. Described as "infrequent and uneven," over half of public schools in the United States provide no cybersecurity education, with most educators identifying areas like cyber law, cryptography, and artificial intelligence as entirely absent (Chiosea, 2020).

Projections estimated a global shortfall of 1.8 million cybersecurity positions by 2022 (Pinchot et al., 2020). Instead, the global workforce gap reached upwards of 3.4 million even while adding nearly a half million jobs in the previous year ((ISC)^2, 2022). Consequently, tremendous effort has been placed on workforce pipelines and cybersecurity education to address the workforce gap and to develop a more cybersecure population. Wagner (2023) examines cybersecurity education frameworks, platforms, and workforce pathways, emphasizing an established need for all-level, all-domain approaches. Useful among these is the *K-12 Cybersecurity Learning Standards* (Cyber Innovation Center & CYBER.ORG, 2021), with focuses on computing systems, digital citizenship, and security. These themes or concepts are further broken down into sub-concepts, topics, and "gradebands" for age-appropriate examples and clarification. We will return to the implementation of these standards shortly.

While much cybersecurity education research demonstrably focuses on business and workforce development, humanistic or philosophical approaches are generally relegated to the realm of ethics. Ethics–specifically cyberbullying–is a frequently addressed topic in K-12 cybersecurity education (Chiosea, 2020). Beyond ethics at one end and purely technical areas like network communications on the other, a vast range of fields and topics are worthy and need investigation and analysis. In the following pages, one approach–an applied postphenomenology–is presented as a robust addition to the methodological toolbox allowing delving deep into the lived experiences associated with technology and the cyber domain, as well as varied pedagogical approaches.

3. PHENOMENOLOGY AND TECHNOLOGY

Prior to exploring *post*phenomenology, we must explore phenomenology itself. Phenomenology is generally known as the philosophical approach to understanding *being in the world* and the experiences therein. It is a wholly qualitative approach, attempting to expose a pure, unvarnished, raw experience and learn from it. In this way, "doing" phenomenology (and postphenomenology, as we will see) is a unique approach to revealing how one is situated within the lifeworld.

Phenomenology can be thought of as "a radical, anti-traditionalist style of philosophizing [seeking] to avoid all misconstructions and impositions placed on experience in advance" (Moran, 2000, p. 4). It is a method of identifying themes across diverse experiences and of making known the connections between what *is* and how it is *perceived to be*. As such, one's intention plays a key role, with the overarching goal being "to discover and describe consciousness by means of studying the essential conscious elements, acts, structures, and their interrelation" (Gutland, 2018, p. 10).

While a full and comprehensive introduction to phenomenology is outside the scope of this paper, a brief venture into a classic example with

technology is warranted: generally, technology is seen as something to overcome. Phenomenology points to the difference between technology working as intended and technology hindering one's actions. The carpenter's hammer is *Zhuhanden*, or *ready-to-hand*, representing the tool as a functional extension of the self (Heidegger, 1927). A carpenter using a working hammer does not direct her intention to the hammer; rather, she directs it to the *nail*. Conversely, a technology that *does* become a hindrance (*Vorhanden*, or *present-at-hand*) no longer expands one's abilities and self but rather is *dealt with*, a situation to overcome (Blitz, 2014). Even if that hammer is ready-to-hand (usable to hammer a nail), it holds the potential to become present-at-hand (a paperweight) at any time.

Postphenomenology turns this on its head, positing that rather than *hindering* experiential understanding, technology instead *mediates* it, worthy of empirical analysis. This is the first step toward the cybersecurity and cybersecurity education connection, which requires deeper exploration.

4. POSTPHENOMENOLOGY

Postphenomenology is presented as the anti-essentialist, empirical, pragmatic methodological successor of phenomenology (Ihde, 1990) and can be defined as a "phenomenology that attends to specific technologies and the existential and epistemological differences they may be making to the lifeworld" (Adams & Turville, 2018, p. 4). It reconsiders technology not as a barrier or hindrance but an invitation through reifying phenomenology's focus on intentionality.

Ihde (1990) initiated the field, describing four core relations between humans, technology, and the world. These describe how amalgams of human-and-technology and technology-and-world are understood, and the direction and path of intention. These are provided alongside typograms for illustration below, along with examples in cybersecurity education to assist in drawing practical connections between the methodology and the domain.

The *embodiment* relation is one in which the human and technology function as one with intention directed at the world:

(Human - Technology) → World

Or, in the case of the carpenter,

(Carpenter – Hammer) → Nail

The carpenter-hammer unit directs intention at the nail. In a cybersecurity context, this is easily understood as user-keyboard directing intention to a website or application. Likewise, it could be explored as user-software directed at a network. The I/technology/world antecedents are malleable, as we will see shortly.

The second relation is the *hermeneutic*, a translatory and interpretational relation, such as reading the time from a clock or examining an x-ray. The user directs their intention toward the technology that, itself, represents something about the world.

Human → (Technology - World)

The interpretive nature of this relation is ostensibly based on trust–one trusts the clock to not be fast or slow–but can lead to unexpected or undesirable outcomes, such as instrumental error resulting in ill-advised decisions (a radar altimeter in a helicopter providing an incorrect distance to the ground, for example). In the cyber domain, one can easily apply this to interpreting network traffic to understand atypical behavior or interpreting email content to identify phishing.

Alterity is the treating of technology as "other." Mundane as a blender or advanced as anthropomorphized digital assistants, it is engaging technology as a separate entity. Like Alexa, where the alteric nature of the interaction is clear (as one would speak to another), the same core relation describes the use of a battery, a safety harness, or lawnmower. With the growing popularity and use of large language models (LLMs) like ChatGPT (OpenAI, 2023), understanding this relation becomes crucially important.

Human → Technology – (– World)

In a cyber context, for example, this could be simply interacting with tools like USB drives or IoT devices.

Finally, the *background* relation deals with technology that, while having a direct impact, is part of the environment. An air conditioner, for example, or smart lights. It is typically the breakdown–becoming *present-at-hand*–of these technologies that bring awareness of their existence and use to the foreground. They are represented as:

Human – (Technology / World)

For the average user, most engagement in the cyber domain appears relegated to the background: security breaches, on-path attacks, unencrypted data transfer, and so on.

Technic relations are not mutually exclusive; rather, they frequently overlap. When driving a vehicle, one embodies the machine as they *feel* the road beneath them through the controls, interprets the speed via the speedometer, works the steering wheel and pedals as alteric tools.

As technologies grow more advanced and permeating more aspects of our lives and bodies, other relations are needed. Peter-Paul Verbeek (2008a; 2015) has expanded these relations through continuing research on technological mediation theory and the concepts of *hybrid* and *composite* intentionalities. These in turn lead to new technic relations beyond Ihde's original four (see Table 1 below):

Cyborg / Fusion	(Human / Technology) → World
Composite	Human → (Technology → World)
Immersion	Human ← → Technology / World
Augmentation	(Human – Technology) → World → (Technology – World)

Table 1: Hybrid and Composite Intentionalities

The "cyborg" or "fusion" relation is typified by a pacemaker: human and machine combine in such a way that one does not function meaningfully without the other. The "composite" relation progresses the hermeneutic relation in that "humans are directed here at the ways in which a technology is directed at the world" (Verbeek, 2008a, p. 393), like a thermal camera displaying what *it* sees that we cannot. An "immersion" relation is akin to the background relation with the difference being the intention is bi-directional (a "smart mirror," for example, fusing technology with the world around it, while reactions become mutual). The "augmented" relation describes a feedback loop: through augmented reality glasses, for example, the user and the glasses are directed toward the world, at which point the glasses "react" to the world, feed that information back to the user, and the user then reacts to *that*.

Identified in these four newer relations, the distance between technologies and the self, approaches zero (i.e., background → immersion, or embodiment → cyborg) and the need to understand new mediation grows in tandem. As stated at the outset, since *all* cybersecurity and cybersecurity education revolve around interactions between humans and/though technology, the need for a deep, meaningful understanding cannot be overstated. And, while "cyborg cybersecurity" may seem relegated to edge cases in medicine or even science fiction, our submergence in the digital realm points toward a growing and inescapable importance. By applying postphenomenological methodology, access to and understanding of this may grow in unexpected ways.

5. APPLIED POSTPHENOMENOLOGY

A variety of postphenomenological accounts of wide-ranging technologies and mediated experiences have been performed in recent years, such as a parent encountering a child through an ultrasound scan (Verbeek, 2008b), an exploration of the world through cochlear implants (Besmer, 2012), even an examination of park benches (Rosenberger, 2020). Lacking dogma, the method for approaching these studies vary as much as their topics. That said, as we mean to apply postphenomenology to cyber and cyber education, three concepts need described: multitstability, transparency, and variational analysis. Combined, these make up a large portion of the postphenomenologist's toolbox.

Technologies have multiple uses. Some uses are easily identified and implemented (an *affordance*, the ways technologies invite a particular use; a doorknob *affords* turning). In postphenomenological terms, this is *sedimentation* (Rosenberger, 2009). A basketball affords a variety of uses but bouncing is *highly sedimented* and is its *dominant stability*. However, a postphenomenological analysis strives to find the *multistability* of a particular technology. How could it be used otherwise? What could it mean? How does it allow new experiences, intended or otherwise? The multistability of technologies is at the core of postphenomenology (see Ihde, 2012).

Transparency (Ihde, 1990), then, can be understood as the degree to which a technology recedes into the background during use. The conscious manipulation or awareness fades and one's intention flows effortlessly to its ultimate target. Driving a car or touch-typing on a keyboard, for example. This is closely related to "field composition" or "field of awareness" (Rosenberger & Verbeek, 2015, p. 23), in which

one's perception shrinks, narrows, or perhaps simply focuses, such as no longer noticing what happens beyond the edges of the screen when viewing a film.

The method of exploring and answering these questions is the most fundamental of postphenomenological methods: variational analysis (literally, analyzing the variations in the ways a technology is used and mediates experience). This is precisely the process that exposes multistability through imagining, experimenting, or investigating the uses of technologies. Rosenberger (2020) describes a next-step: variational cross-examination, allowing us to "learn things *about particular stabilities* through their comparison *with one another*" (p. 6; emphasis in original). He elaborates:

> …it can be especially difficult to investigate a dominant stability (whether through postphenomenology or any other perspective). It calls for an effort to see through normalcy, to extract things from their contexts (at least provisionally), to look past many specific design elements, and to break potentially deeply-ingrained habits of perception and understanding. The postphenomenological method of variational cross-examination can be useful for this kind of project. (p. 6)

Still, though we have examples of cases and methodological steps to take, how precisely does one *do* postphenomenology? How to implement this approach needs to be unpacked before doing the application. Adams & Turville (2018) provide something of a roadmap for practicing this philosophy of technology in education, stemming from van Manen's *Phenomenology of Practice* (see Van Manen (2014)). "The ambition of phenomenology of practice is simple: to describe and reflect on a phenomenon of professional or personal interest by attending to the prereflective or everyday lifeworld" (Adams & Turville, 2018, pp. 11–12). Through these approaches, we begin to tease out the ways in which postphenomenology may shed light on a complex, multifaceted domain like cyber. Concrete steps for variational data generation–that is, how one might go about gaining access to these stabilities–are described below.

Bringing this phenomenology of practice into a *post*phenomenology of practice (or, an "applied postphenomenology") strives for "thematizing of materiality, particularly in the form of instruments and devices which we make 'worlds' available to us which were previously unexperienced and unperceived" (Ihde (2003) in Adams & Turville (2018)). Specifically, one must generate data for a postphenomenological analysis, as with any research. Four methods of phenomenology of practice and postphenomenological data generation described by Adams and Turville are outlined below. Explicit ties to a postphenomenology of cybersecurity education are described in the section following.

1. **Prereflective: self-observational anecdotes**. A method relying on the observer to describe, with a distanced kind of clarity and lack of judgment, her own "concrete, lived-through" experiences.
2. **Prereflective: interviews**. Interviews, but specifically with a goal to "elicit lived experience descriptions (LEDs) about the research participant's everyday engagements and encounters with the technology of interest" (Adams & Turville, 2018, p. 15).
3. **Prereflective: observational anecdotes**. Observing the experiences of others is yet another method. This method may lack a certain depth provided by others but may equally lead to accessing experiences and uses of technologies of which users themselves may be unaware.
4. **Reflective: the breakdowns**. Reflecting on technological breakdowns naturally demonstrates and brings to light its multistability and stabilities, while exposing it to meaningful variational analysis. More simply: what happens when the tool breaks, and what could it tell us about the tool, ourselves, and the person-tool-world amalgam?

Key here follows Verbeek's insistence that intentionality "needs to be understood as the specific ways in which specific technologies can be directed as specific aspects of reality" (2008a, p. 6). This provides an opening to understanding how this methodology could be applied to cybersecurity and cybersecurity education. With these four approaches to applying postphenomenology to specific situations, combined with the variational analysis and cross-examination methods, we may explore practical applications. These methods may sound familiar upon reflection. Indeed, while phenomenological approaches to exploring cybersecurity–especially deception–exist (see Majkut et al. (2009)), explicit *post*phenomenological explorations of cybersecurity and cybersecurity education are missing from the literature. First, though, we will explore postphenomenological applications

outside the cyber domain to assist in making the jump.

6. PRACTICAL APPLICATIONS

Postphenomenological explorations involve considerable creative exploration and observation of people's lived experiences. Prior to attempting concrete connections to cyber and cybersecurity education, there is value to *priming the pump*, as it were, by delving into existing postphenomenological applications across domains.

Postphenomenological approaches can been seen ranging in research on fitness, especially the technological methods of tracking fitness (Ayas Önol & Akyaman, 2021; Zheng, 2021), to ethics (Morrison, 2020; Verbeek, 2023). The medical field has been especially ripe for postphenomenological analyses, whether these are the sonographic experiences parents have of the fetus in utero (Verbeek, 2008b) or analyses of assistive technology used by older people (Lynch et al., 2022).

Attempts to bring the benefits and insights provided by postphenomenological analysis to the development of other frameworks have also been made. For example, Vindenes and Wasson (2021) provide a postphenomenological framework for studying virtual reality and user experience, describing a "simulated subjectivity" that, through technologically-mediated immersive experiences, can lead to promoting empathy and revealing "otherness."

Research in education has benefitted from postphenomenological application, such as Wellner & Levin's (2023) focus on Papert's constructionist pedagogical framework, drawing insightful and explicit connections between the "four qualities" of learning environment personalization (embodiment), computational thinking (hermeneutics), microworlds (alterity), and the democratization of education (background relations). Likewise, the work of Adams & Turville, which is referenced here at length, provides actionable approaches to marrying postphenomenology and pedagogy, leading to a "posthuman inquiry" method.

The myriad fields postphenomenology can be applied to are demonstrably as numerous as the ways to apply it. Understanding these while having concrete examples of postphenomenological studies makes for a smoother integration into the cyber domain, cybersecurity education, especially.

7. POSTPHENOMENOLOGICAL CYBERSECURITY AND EDUCATION

Adams & Turville (2018), in *Doing Postphenomenology in Education*, demonstrate precisely why this particular methodology is relevant and applicable in this context: it "involves attending to the unique differences a particular technology makes to teaching practice, knowledge apprehension, and pedagogical meaning" (p. 20). When "…my email tugs at me to check it, my buzzing iPhone insists that I answer it" (Adams & Turville, 2018, p. 12), the relationship between self and technology determines the reaction. Typically, it is steeped in trust, familiarity, even muscle memory. The question arises: should this be the case and what implications does this have for education in the cyber domain?

First, an example in cybersecurity education: for a learner first presented with **nmap**, the network mapping tool, what does the blinking cursor invite? When the search begins, the learner no longer maintains a meaningful dichotomous distinction from the computer. While they may be *treating* the computer as alteric, the learner's machine itself recedes into the background as they beings to embody the interface, a **user-nmap** hybrid. Much as Ihde experiences the chalkboard through the chalk or Heidegger's carpenter experiences the nail through the hammer, the learner is experiencing the network landscape through the keyboard and screen, the capabilities of the software, and their familiarity with each system involved. We can now see the range of postphenomenological components at play: the multistability (computer-as-productivity-tool versus computer-as-attack-surface) and transparency (the learner embodies the keyboard and the software) of the hardware. As in traditional phenomenological analysis, uncovering the hidden stabilities in the complex network of devices and intent can be prohibitively difficult. The process takes practice.

This difficulty (or, optimistically, opportunity) is partly due to the lack of any "strict postphenomenological methodology that scholars could follow. Postphenomenology comes in just as many flavors as there are scholars in the field" (Rosenberger & Verbeek, 2015, p. 2). This results in an openness allowing cybersecurity researchers and educators to explore the possibilities presented here. Variation and multistability in the world of cybersecurity is ever-present: a website exploit is a prime example. A feature in a website with a particular intended function can be used for something unintended,

often nefarious. The phrase, "It's a feature, not a bug" is itself a description of a technology's multistability and a reflective breakdown analysis. Postphenomenological tools like variational analysis are key in uncovering not just multistabilities, but even revealing the technologies, themselves. Teaching learners to approach the cyber domain with these relations in mind can help them engage in "phenomenological looking" (Ihde, 2012), unveiling experiences they are having but unaware of.

Returning to the K12 Cybersecurity Standards Learning Standards (2021), we see how one might use postphenomenological methods to explore and instruct. Concretely, **K-2.DC.THRT**, "Describe good and bad uses of digital devices" is precisely a variational analysis. Consider how photography is specifically identified in the gradeband standard: variational analysis of this leads to the revealing of photo "tagging" on social media as both a space for community building and memory-making, while also potentially being a place for ridicule, ostracization, or harassment (for detailed examples of this approach, see Rosenberger (2020) for bench-as-library and bench-as-political-statement). Similarly, the "Digital Footprint" standards like **6-8.DC-FOOT.2**, "Recognize the permanence of a digital footprint," suggests "digital heaviness" (O'Neal Irwin, 2018), a weight felt when private moments are digitally exposed publicly.

8. LIMITATIONS

While taking a postphenomenological approach to the cyber domain and cybersecurity education may indeed expose new concepts, experiences, and considerations, the methodology is not without its limitations. Primarily, the practical application of postphenomenological methods can be a significant hurdle for educators and researchers.

Postphenomenology has been criticized for lacking a mechanism to explore systemic issues and instead focusing entirely on individualized experience. Arzroomchilar (2022) draws attention to the postphenomenological tendency to ignore the historical context of a technology and the "debates, disputes and fights" (np.) accompanying it, as well as the omission of social and political analyses inherent in the framework. Aagaard (2017) likewise points out the range of feminist critiques and responses in the literature surrounding issues of the politicization of experience and the natural discourse surrounding the use of technologies. Especially in the cyber domain, future research and analysis into these critiques would provide a more robust framework.

9. CONCLUSION

In the preceding pages, I have attempted to draw meaningful connections between traditional phenomenology, the technologically focused postphenomenology, ways one may "do" postphenomenology in the cyber domain, and the need for and application of those methods in cybersecurity and cybersecurity education. While there is no hard-and-fast walkthrough for engaging in a postphenomenological study, I have presented a variety of methods to apply and tools to use, most notably those of variational analysis to reveal a technology's multistability, and the prereflective and reflective approaches of the postphenomenology of practice. Examples of postphenomenological studies have also been highlighted along with criticisms and suggestions for future study.

This leaves avenues to explore. The most relevant to cybersecurity and cybersecurity education may be that of the present understanding and confines of the complex intentionalities involved. Within the cybersecurity domain, it's entirely possible the postphenomenological intentionality landscape may need expanded to account for common situations like on-path attacks (a "sabotage intentionality," perhaps, to describe the injection of a bad actor's intent into a victim's experience). This is precisely why postphenomenology may prove exceedingly fruitful in cybersecurity education: focusing on the potentially conflicting intentionalities and mediations present in the cyber domain may make possible the moving beyond what is often a transactional and purely technical venture. Some, like Blair et al. (2020) and Austin (2020), point explicitly to the need for wholesale reconsideration of the nature of cybersecurity education, suggesting the need for–in contrast to the frequent autodidacticism seen presently–holistic and institutional research-based approaches, respectively. Crucially, a postphenomenological approach may be a solution to Blair et. al.'s challenge that "cyber should also be addressed when covering most of the social sciences (such as political science, economics, international relations, and sociology) as well as in law, ethics, and social justice components, and in studies of human behavior" (p. 5), given the infusion of technology into all spaces.

In fact, there is no shortage of opportunities to apply a postphenomenological approach to

cybersecurity and cybersecurity education: one could delve deep into competitions held by various cybersecurity organizations like the National Cyber League, explore spam email and what we can learn about how it is experienced differently between users, perform variational analyses in a penetration testing course on any of the range of software bundled in Kali Linux. If technology is involved, researchers and educators may attempt applying postphenomenology to uncover those heretofore unseen stabilities.

As such, this paper is intended to build a foundation for postphenomenological explorations into the cybersecurity and cybersecurity education domains. Of particular and timely importance is the sudden and ubiquitous appearance of generative AI like ChatGPT (OpenAI, 2023) and the extraordinary ways this technology will influence all domains, not just those discussed here. For example, the recent release of WormGPT, a "blackhat alternative" to ChatGPT and other generative text systems (*WormGPT*, 2023), presents a meaningful and worthwhile subject for postphenomenological analysis. Future research is invited to further act on the postphenomenological approach and find the as-yet unseen ways these technologies influence more than just education.

10. REFERENCES

Aagaard, J. (2017). Introducing postphenomenological research: A brief and selective sketch of phenomenological research methods. *International Journal of Qualitative Studies in Education*, *30*(6), 519–533. https://doi.org/10.1080/09518398.2016.1263884

Adams, C., & Turville, J. (2018). Doing Postphenomenology in Education. In J. K. B. Friis, J. Aagaard, J. Sorenson & O. Taldrup (Eds.), *Postphenomenological Methodologies: New Ways in Mediating Techno-Human Relationships* (pp. 3–25). Lexington Books.

Arzroomchilar, E. (2022). Some Suggestions to Improve Postphenomenology. *Human Studies*. https://doi.org/10.1007/s10746-021-09615-1

Austin, G. (2020). Twelve dilemmas of reform in cyber security education. In G. Austin (Ed.), *Cyber Security Education*. Routledge.

Ayas Önol, T., & Akyaman, S. (2021). "What's The Point of Exercising If It Cannot Be Measured?" A Post-Phenomenological Analysis of Self-Tracking Devices. *AGATHOS*, *12*(2), 7–23. https://www.agathos-international-review.com/issue12_2/03.Onol%20&%20Akyaman.pdf

Besmer, K. (2012). Embodying a Translation Technology: The Cochlear Implant and Cyborg Intentionality. *Techné: Research in Philosophy and Technology*, *16*(3), 296–316.

Blair, J. R. S., Hall, A. O., & Sobiesk, E. (2020). Holistic cyber education. In G. Austin (Ed.), *Cyber Security Education*. Routledge.

Blitz, M. (2014). Understanding Heidegger on Technology. *The New Atlantis*, *41*, 63–80.

Chiosea, F. (2020). *The State of Cybersecurity Education in K-12 Schools*. EdWeek Research Center. https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf

Cyber Innovation Center, & CYBER.ORG. (2021). *K-12 Cybersecurity Learning Standards*. https://cyber.org/standards

Gutland, C. (2018). Husserlian Phenomenology as a Kind of Introspection. *Frontiers in Psychology*, *9*.

Heidegger, M. (1927). *Being and Time* (2010 translation). State University of New York Press.

(ISC)². (2022). *(ISC)² 2022 Cybersecurity Workforce Study*. https://www.isc2.org/Research/Workforce-Study

Ihde, D. (1990). *Technology and the Lifeworld: From Garden to Earth*. Indiana University Press.

Ihde, D. (2003). Postphenomenology - Again? *Working Papers from the Centre for STS Studies, University of Aarhus*, (3).

Ihde, D. (2012). *Experimental Phenomenology: Multistabilities* (2nd ed.). State University of New York Press.

Irwin, S. O. (2018). The Unbearable Lightness (and Heaviness) of Being Digital. In A. Romele & E. Terrone (Eds.), *Towards a Philosophy of Digital Media* (pp. 185–203). Springer International Publishing.

Lynch, J., Hughes, G., Papoutsi, C., Wherton, J., & A'Court, C. (2022). "It's no good but at least I've always got it round my neck": A postphenomenological analysis of reassurance in assistive technology use by

older people. *Social Science & Medicine, 292*, 114553. https://doi.org/10.1016/j.socscimed.2021.114553

Majkut, P., Carrillo Canan, A. J. L., Basch, C. A., Conde, O., Dalke, T. P., Egan, K. S., Borup, T., Bourdaa, M., & Cline, K. (2009). On deception: A phenomenological approach. In P. Majkut & A. J. L. Carrillo Canan (Eds.), *Deception: Essays from the Outis Project on Deception*. Zeta Books.

Moran, D. (2000). *Introduction to Phenomenology*. Routledge. https://arxiv.org/abs/0712.0689

Morrison, L. A. (2020). Situating Moral Agency: How Postphenomenology Can Benefit Engineering Ethics. Science & Engineering Ethics, 26(3), 1377–1401. https://doi.org/10.1007/s11948-019-00163-7

OpenAI. (2023). *ChatGPT*. https://chat.openai.com

Pinchot, J., Cellante, D., Mishra, S., & Paullet, K. (2020). Student Perceptions of Challenges and Role of Mentorship in Cybersecurity Careers: Addressing the Gender Gap. *Information Systems Education Journal (ISEDJ)*, *18*(3), 44–53.

Rosenberger, R. (2009). The habits of computer use. *International Journal of Computing & Information Technology*, *1*(1), 22–28.

Rosenberger, R. (2020). On variational cross-examination: A method for postphenomenological multistability. *AI & SOCIETY*. https://doi.org/10.1007/s00146-020-01050-7

Rosenberger, R., & Verbeek, P.-P. (2015). A Field Guide to Postphenomenology. In R. Rosenberger & P.-P. Verbeek (Eds.), *Postphenomenological Investigations: Essays on Human-Technology Relations* (pp. 9–41). Lexington Books.

Van Manen, M. (2014). *Phenomenology of practice: Meaning-giving methods in phenomenological research and writing*. Left Coast Press.

Verbeek, P.-P. (2008a). Cyborg intentionality: Rethinking the phenomenology of human-technology relations. *Phenomenology and the Cognitive Sciences*, *7*(3), 387–395.

Verbeek, P.-P. (2008b). Obstetric ultrasound and the technological mediation of morality: A postphenomenological analysis. *Human Studies*, *31*(1), 11–26. https://doi.org/10.1007/s10746-007-9079-0

Verbeek, P.-P. (2015). Toward a Theory of Technological Mediation. In J. Kyrre Berg Friis & R. P. Crease (Eds.), *Technoscience and Postphenomenology: The Manhattan Papers*. Lexington Books.

Verbeek, P.-P. (2023). Postphenomenology and Ethics. In *Technology Ethics*. Routledge.

Wagner, P. (2023). CyberEducation-by-Design. *Cybersecurity Pedagogy and Practice Journal*, *2*(1), 50. https://cppj.info/2023-2/n1/CPPJv2n1p50.htm

Wellner, G., & Levin, I. (2023). Ihde meets Papert: Combining postphenomenology and constructionism for a future agenda of philosophy of education in the era of digital technologies. *Learning, Media and Technology*, 1–14. https://doi.org/10.1080/17439884.2023.2251388

Vindenes, J., & Wasson, B. (2021). A Postphenomenological Framework for Studying User Experience of Immersive Virtual Reality. *Frontiers in Virtual Reality*, 2, 656423. https://doi.org/10.3389/frvir.2021.656423

WormGPT: New AI Tool Allows Cybercriminals to Launch Sophisticated Cyber Attacks. (2023). The Hacker News. https://thehackernews.com/2023/07/wormgpt-new-ai-tool-allows.html

Zheng, E. L. (2021). Interpreting fitness: Self-tracking with fitness apps through a postphenomenology lens. *AI & SOCIETY*. https://doi.org/10.1007/s00146-021-0114